카이버네트워크

신용 검증 필요 없는 탈중앙화된 환전과 지불 서비스

로이 루(Loi Luu), 야론 벨르너(Yaron Velner)
[loiluu, yaron.velner]@kyber.network
(v0.7, 2017.7.5 등록됨)

초록: 우리는 디지털 자산(예. 암호화 토큰)과 암호화 화폐(예. 이더, 비트코인, 지캐쉬)들 간에 높은 유동성으로 즉각적인 환전 및 변환을 하는 블록체인상의 프로토콜인 카이버네트워크를 설계하고 구축한다. 카이버네트워크는 다음의 몇가지 이상적인 특징을 구현할 첫번째 시스템이다. 1) 신용을 검증할 필요가 없는 환전(암호화 화폐 교환), 2) 분산화된 실행, 3) 즉각적인 거래와 높은 유동성. 카이버네트워크는 환전 서비스 뿐만 아니라 지불 API들을 통해 이더리움 계좌가 쉽게 다른 암호화 토큰들로 지불 받을 수 있게 할 것이다. 일례로 이제 카이버네트워크 API들을 사용하여 어떤 판매자도 구매자가 아무 암호화 토큰으로도 지불 가능하게 할 수 있다. 그러면 판매자가 실제로 지불 받을 때는 이더(ETH)나 판매자가 선호하는 다른 어떤 토큰으로도 받을 수 있다.
카이버네트워크는 이더리움 네트워크에서 먼저 운용될 예정이며, 상호 다른 블록체인의 암호화 화폐간 거래에도 폴카닷(Polkadot)이나 코스모스(Cosmos)와 같은 추후 구현될 중계 프로토콜을 사용하여 지원하는 것이 카이버네트워크 개발 로드맵 상에 포함되어 있다. 신용 검증 필요 없는 지불 서비스들을 통해, 비트코인(Bitcoin), 지캐쉬(ZCash), 그리고 다른 암호화 화폐에서 이더리움 계좌로 우리의 결제 API들로 안전하게 지불 받는 것이 가능하다. 카이버네트워크 크리스탈스(KyberNetwork Crystals;KNC)와 선택된 암호화 화폐 사용자들을 위해 변동성 위험에 대한 노출을 완화하기 위한 파생금융상품이 소개될 것이다. 이것은 사용자들이 종합적인 가격 움직임에 참여할 수 있도록 한다.

목 차

1. 서론

비트코인, 이더리움과 같은 떠오르는 암호화 화폐들은 최근에 힘을 얻고 있다. 왜냐하면 그것들은 사용자가 그들의 디지털 자산들을 거래 및 관리할 때 탈중앙화되고 신용 검증 필요 없는 모델을 사용할 수 있게 하기 때문이다. 더욱 재미있는 것은 이더리움 네트워크는 튜링 완전 스크립트 언어와 신용 검증 필요 없는 스마트 컨트랙트의 기능을 가지고 있다. 이것으로 실제 현물 자산과 연동되거나(예. 디직스 골드 토큰; 금과 연계된 토큰) 가치를 담고 있는 플랫폼(예. 골렘네트워크 토큰, 그노시스 토큰, 어거 토큰, 기타 등등)에 대한 자신들의 암호화 토큰들을 발행하고 디지털화 하기 쉽게 만든다. 지금까지 가장 유명한 암호화 화폐의 전체 시가 총액은 720 억 달러[1]이다. 이 전체 시총은 지난 5 개월 동안 3 배가 되었고 계속해서 성장하고 있다.

1.1. 동기

1.1.1. 중앙 집중화의 위험성

블록체인 시장이 성장하고 많은 암호화 자산들이 등장함에 따라, 암호화 토큰 간의 환전과 변환에 대한 수요가 언제나 증가하고 있다. 그 예로 주요 거래소의 이더와 비트코인간의 환전거래량은 하루에 수억 달러에 육박한다. 이더와 이더리움 네트워크의 암호화 토큰 간(대부분 발행된 지 2 년이 안된)의 총 거래량은 약 백만 달러에 달한다. 그럼에도 불구하고, 탈중앙화되고 신용 검증이 태생적으로 필요 없는 암호화 화폐 또는 암호화 토큰들은 대부분 중앙화되고 내부 사기와 외부 해킹에 취약할 수 있는 거래소에 의해 거래가 되고 있다. 이것은 계속해서 영향을 미치고 있고 다양한 거래소[2]들에서 많은 해킹 사건들이 보고되었고 이것은 무수한 사용자들에게 피해를 끼치고 수억 달러의 돈을 잃게 만들었다.

1.1.2. 부족한 즉각적인 환전

기존의 환전들은 사용자들이 그들의 돈에 대한 출금 인가을 받기 전 자주 몇 분 이상을 기다려야 했다. 이것은 중앙집중화되거나 탈중앙화된 것 모두 해당되었다.

1.1.3. 현존하는 분산화된 거래소의 문제점

탈중앙화된 거래소를 구축하는 일은 이더리움 네트워크[3]의 몇몇 참여자들에 의해 개시되었다. 이들이 탈중앙화되고 신용 검증 필요 없는 거래소를 만들었더라도, 그들은 여전히 외부 주가 조작에 취약하다. 왜냐하면 거래 주문은 블록에 기록되는데, 거래 주문이 만들어지는 것과 블록이 생성되는 것은 시간차가 있기 때문이다. (더 자세한 것은 이곳에)
기존의 분산화된 거래소가 의도대로 동작하지 않는 것은 또 다른 원인들이 있다. 이 거래소들은 사용자의 주문 장부를 블록체인에 보관한다. 그 결과로 거래의 주문 수정과 주문 취소 명령 자체에 대한 비용이 비싸질 수 있다. 매도 주문과 매수 주문간의 가격이 맞춰질 때 까지 비용이 올라갈 것이고 반복된 주문 수정은 그것을 더욱 악화 시킬 것이다.
한 거래소[4]는 이 문제를 해결하기 위해 가격을 맞추고 협상하는 과정을 오프라인에서 중개자를 거쳐서 진행하기를 희망한다. 거래는 두 거래 당사자가 환전 비율에 동의를 한 후에만 블록체인

---

[1] https://coinmarketcap.com/charts/

[2] 예를 들면, 마운트곡스(MtGox), 비트파이넥스(Bitfinex), 쉐이프쉬프트(Shapeshift).

[3] 이더리움 기반 거래소는 다음 사례들이 있다. 0xProject, OasisIndex 및 EtherDelta.

[4] Swap.tech

상에서 이루어진다. 이것은 중개자가 최고의 상대 거래 당사자를 찾아주는 것에 대해 신뢰 문제가 생길 수 있다. 우리는 또한 수수료 없는 주문들은 적대적 사이블 공격(역자주: 여러 ID 를 이용한 시스템 또는 네트워크 공격)과 서비스- 거부 공격(역자주: 대량의 쓰레기 트래픽을 일으켜 서버와 네트워크를 일시적 사용 불능의 상태로 만드는 공격)에 취약한 것에 주목한다.

1.1.4. 여러 디지털 자산을 가지는 것에 대한 문제점

ICO 의 수가 증가함에 따라, 많은 수의 새로운 암호화 토큰들이 나타났다. 이성적인 추론으로 투자자들은 투자 전략의 일환으로 다양한 암호화 토큰들을 가지려 할 것임을 알 수 있다. 하나의 암호화 토큰을 다른 암호화 토큰으로 교환하는 것은 투자자와 운영자 모두에게 새로운 도전과제이다. 예를 들어, 이미 적용된 계약에 새로운 암호화 토큰을 결제 방법으로 허용하는 것은 모든 거래 당사자들에게 어려운 일이다.
암호화 토큰들이 많아지면 버그와 보안적 결함이 생길 수 있는 공간이 많아 진다. 예를 들면, 최근에 DAO 토큰 ICO 에서는 같은 정도의 금액으로 투자했음에도 불구하고 이더로 투자한 투자자보다 SNGLS(역자주: SingularDTV 의 토큰)로 투자한 투자자가 더 많은 토큰을 부여 받는 중대한 버그가 발견되었다. 따라서 이런 상황에서 네트워크 내의 토큰 보유자, 판매자 및 사용자에 대한 지불 절차를 단순화 할 필요가 있다.

1.2. 카이버네트워크

우리는 카이버네트워크를 소개한다. 이는 블록체인 상의 탈중앙화된 환전을 제공하며, 실제 환전 기능을 구축하고 판매자와 사용자를 위한 유용한 결제 API 들을 제공하여 즉각적인 토큰 변환을 쉽고 신용 검증이 필요 없게 하는 것이 특징이다. 여기에 주문 장부는 없다. 사용자들은 거래를 하기 전에 환율을 알고 그에 해당하는 금액을 받게 될 것이다. 사용자들은 어떤 추가 수수료도 지불하지 않는다(거래 자체에 대한 가스 수수료는 제외). 카이버네트워크는 환율의 합리적인 전파를 통한 가격 책정으로 이익을 발생시킨다.

우리의 사용자는 그들의 기존의 토큰 A 를 다른 토큰 B 로 변환하여 토큰 B 로만 받는 다른 사용자에게 보낼 수 있다. 더 재미있는 것은 카이버네트워크의 새로운 표준 계약 지갑은 기존의 단 몇 종류의 토큰만 받는 다른 계약을 허용한다. 또한 계약 코드에 어떤 수정도 하지 않고 미래의 어떤 토큰으로도 지불 받을 수 있다. 이것은 계약이나 판매자가 더 넓은 계층의 사용자에게서 카이버네트워크가 지원하는 어떠한 토큰으로도 지불 받거나 투자 받을 수 있게 한다.

카이버네트워크의 설계에는 이러한 모든 응용 프로그램을 지원하는 몇가지 새로운 구조가 있다.

- 글로벌 주문 장부를 운용하는 대신, 우리는 환전 유동성을 유지하기 위해 적절한 양의 암호 토큰을 보유하는 예비 창고를 운용한다. 이 보유분은 카이버 계약에 의해 직접 제어되며, 그 계약에는 모든 보유분과 연결된 각 토큰 교환 쌍의 환율이 있다. 그 환율은 보유분 관리자에 의해 빈번하게 업로드 되며, 카이버 계약은 사용자에 있어 가장 좋은 환율을 선택할 것이다. 토큰 A 에서 토큰 B 로의 환전 요청이 도착하면, 카이버 계약은 정확한 금액의 토큰 A 가 계약서에 입금되었는지 확인한 다음 보낸 사람의 지정된 계좌로 해당 금액의 토큰 B 를 송금한다. 수수료를 제한 토큰 A 의 금액 만큼 토큰 B 를 제공하는 보유분에 적립된다.
- 우리는 새로운 표준 계약 지갑을 통해 우리의 흥미로운 일부 응용 프로그램을 사용할 수 있다. 특히 새로운 표준 계약 지갑을 사용하면 카이버 계약서를 통해 사용자가 새로 변환된 토큰을 사용자를 대신하여 목적지 주소로 보낼 수 있다. 그 대상 주소는 토큰이 카이버 계약에서 보낸 것이 아닌 실제 보낸 사람으로부터 송금 된 것처럼 변환 된 토큰을 받는다.
- 장기 계획에는 EVM 언어의 향후 기능들을 사용하여 이더리움에서 효율적인 지캐쉬 중계를 구축하는 것도 포함된다. 이더리움 안에서의 지캐쉬 중계는 서로 다른 블록체인인 이더와 지캐쉬를 교환하는 것을 가능하게 할 것이다. 우리는 또한 폴카닷 및 코스모스와 같은 미래의 플랫폼을 활용하여 보다 많은 교차 연계 거래 및 지불을 가능하게 한다.

- 카이버 계약은 잘 모듈화 된 구성 요소가 있는 확장성에 초점을 맞추고 설계되었다. 특히 새로운 토큰을 동적으로 추가하거나 기존 토큰을 삭제할 수 있다. 따라서 우리는 앞으로 어떤 토큰이나 디지털 자산과도 작업 할 수 있다.

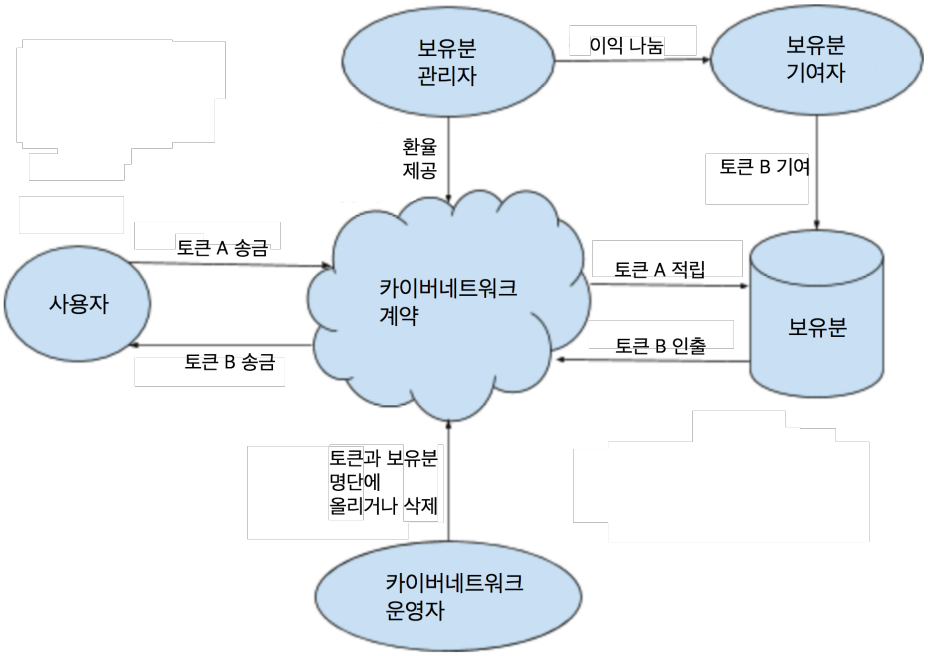
2. 카이버네트워크의 설계

2.1. 카이버네트워크를 운용하는 구성원들의 종류

카이버네트워크에는 5 종류의 역할 구성원들이 있다.

1. 사용자 : 네트워크에서 토큰[5]을 주고 받는다. 카이버네트워크의 사용자는 개별 사용자와 스마트 컨트랙트 계좌 및 판매자를 포함한다.
2. 보유분 개체(들) : 플랫폼에 유동성을 제공한다.
3. 보유분 기여자 : 보유분 개체에 자본을 제공하고 플랫폼 이익을 나눠 갖는다.
4. 보유분 관리자 : 보유분을 유지 관리하고 환율을 결정하여 카이버네트워크에 결정한 환율을 제공한다.
5. 카이버네트워크 운영자 : 네트워크에 보유분 개체들을 넣고 빼거나, 토큰 환전 쌍을 환전 리스트에 추가 또는 삭제하는 책무를 담당한다.

각 구성원들은 스마트 컨트랙트와 독립적인 다른 방식으로 상호 작용한다. 사용자는 한 거래에서 보유분이나 카이버네트워크 운영자로부터 어떤 응답도 기다리지 않고 토큰들을 주고 받는다. 보유분 관리자가 환율을 결정하고 계약에 환율을 제공하는 고정된 시간(수초 기준) 동안 카이버네트워크 운영자는 보유분을 추가하거나 없애는 책무를 수행한다. 주요 계약은 높은 유동성을 보장하기 위해 보유분 개체에 의존한다. 아래 다이어그램은 각 구성원들 간의 상호 작용을 나타낸다.



5 백서의 나머지 부분을 위해 여기서 이 토큰은 이더 화폐도 될 수 있다

2.2. 동적 보유분 풀

카이버네트워크는 네트워크의 기존 보유분을 레버리징하여 높은 유동성을 보장한다. 여러 보유분들은 여러 보유분 관리자들에 의해 직접적으로 관리된다. 이것은 카이버네트워크 운영자와 연관될 수도 있고 되지 않을 수도 있다. 카이버네트워크는 여러개의 부유분들을 활용하여 더 좋은 가격과(보유분 독점을 제거하여) 더 좋은 유동성을 보장(여러 출처를 활용하여)하는 것을 공존 시킨다. 게다가 카이버네트워크 운영자와 상관없는 다른 사람이 자신들의 보유분들을 카이버네트워크에서 관리하여 거래량이 적은 토큰들을 지원할 수 있다. 그 토큰들의 해당 보유분 관리자의 관리 업무량이 분산되고 이것을 대신하여 지원하는 것이다. 따라서 거래량이 적은 토큰을 거래하고 변환하는 위험을 감수하려는 참가자들은 카이버네트워크에 등록하여 그들의 토큰 보유분을 만들 수 있다. 이 때 카이버네트워크는 등록된 보유분들의 어떤 자금도 직접 들고 있지 않는다. 등록된 그들의 자금은 카이버네트워크의 기본 원칙에 입각한 그들의 보유분 계약에 따라 저장된다.

거래/변환이 요청이 도달하면, 카이버네트워크는 그 요청을 처리할 수 있는 모든 보유분에서 토큰 변환 환율을 가져온다. 그런 다음 카이버네트워크는 그 중 가장 최적의 환율을 선택하고 거래 및 변환 요청을 수행한다. 우리는 보유분과 사용자가 모두 안전하다는 것을 보장한다. 즉, 우리는 어떤 참가자들의 자금도 직접 건드리지 않으며 모든 거래는 개별 단위로 나뉜다.

우리는 우리가 카이버네트워크를 런칭할 때 우리가 네트워크에 제공한 단 하나의 보유분만 가지고 있을 가능성이 높다. 이 보유분은 다른 보유분들이 등록되기 전 시스템의 유동성을 위한 주요 기반으로 작용할 것이다.

다른 보유자들이 왜 카이버네트워크에 참가해야하는가? 카이버네트워크는 보유분 관리자가 자신들의 놀고있는 자산들을 통해 수익을 창출 할 수 있는 플랫폼을 만든다. 보유자들은 그들이 결정한 매도 매수 가격 차액으로 사용자의 거래 요청을 처리함으로써 이익을 창출한다. 물론 보유자들은 카이버네트워크에 가입하지 않고도 항상 거래를 할 수 있지만 카이버네트워크의 네트워크 효과로 인해 그들은 더 큰 거래량을 가질 수 있다. 우리는 지갑 서비스 업체들과 다른 토큰 프로젝트들과 협업하여 더 많은 사용자들을 카이버네트워크로 유치할 것이다. 여기에 더해, 카이버네트워크는 보유분 대시보드 소프트웨어도 제공하여 보유분 관리자들이 자신의 보유분 포트폴리오를 관리할 수 있도록 한다. 보유분 대시보드는 보유분 관리자들이 자동으로 가격을 책정하고 자신들의 포트폴리오를 재조정할 수 있는 표준적인 것과 인기있는 거래 알고리즘/전략들이 포함될 것이다. 우리의 보유분 대시보드는 유연성이 뛰어나 보유분 관리자들이 언제 어디서나 자신들에게 맞아 보이는 자신들의 전략들을 항상 구현하고 적용할 수 있다.

어떻게 보유분을 안전하게 지키는가? 보유분에 대한 보안은 카이버네트워크의 주요 관심 분야가 된다. 특히 네트워크의 다른 구성원들로부터 기여를 받는 공개 보유분에 대한 것이다. 주요 고려 사항 중 하나는 나쁜/비윤리적인 보유분 관리자가 다른 보유분으로부터 모든 코인들을 차지하기 위해 나쁜 가격을 호가로 부르고 거래할 수 있다는 것이다.
우리는 보유분을 두가지 타입으로 분류한다:
(1) 외부 기여금을 받지 않는 개인 보유분
(2) 외부 기여금을 받아 기여자들에게 이익을 나누는 공개 보유분
여전히 유효한 주요 고려 사항이지만, 만약 개인 보유분의 보유분 관리자들이 우수한 보안 관행을 따른다면, 개인 보유분의 노출에 대한 위험도는 수용 가능한 범위 내로 한정될 것이다. 왜냐하면 그 보유분들은 지역적으로 처리되고 다른 참가자들은 권한없이 접근할 수 없기 때문이다. 반면, 공개 보유분은 공개성으로 인해 노출에 대한 위험도가 더 높다. 공개 보유분에

대한 보안의 위험을 줄이기 위해 우리는 신용 검증 필요 없는 자금 관리 모델(예. 멜론포트(MelonPort)가 개발한 멜론펀드(MelonFund))을 적용할 것이다. 그를 통해 보유분의 기여자들이 보유분 관리자들의 신용을 검증할 필요가 없도록 한다. 또한 우리는 공개 보유분을 보호하기 위한 제한사항들을 도입할 계획이다. 예를 들어, 보유분의 자금은 자체 보유분 계약에 의해 오직 사전에 협약된 계좌 또는 그 보유분과 상호작용하는 다른 거래소에만 송금가능하다. 따라서 시스템 외부에서 부당하게 자금이 인출될 위험이 사라진다. 또한 보유분 관리자들의 고의적인 허위 및 불합리한 환율을 설정하는 것(예. 전체 시장에서 백만 GNT- 골렘네트워크 토큰 당 하나의 이더의 환율인 상황에서 순간 환율이 오직 500 개 GNT 당 하나의 이더가 되었을 경우 보유분 관리자들은 GNT 를 훨씬 더 싼 가격으로 살 수 있다.)을 막기 위해 우리는 블록체인상의 메카니즘(예. 특별한 권한 없는 비합리적인 가격의 환전)과 블록체인상이 아닌 메카니즘을 모두 적용한다. 예를 들어, 백그라운드 감시자가 시스템이 네트워크의 무결성을 해치는 모호한 활동을 감지했을 때 거래를 중단 시킬 것이고 네트워크의 어떠한 보유분 관리자로부터의 의심스러운 행위를 관찰하고 보고할 수 있다.

2.3. 메인 시스템 구성 요소

카이버네트워크는 시스템에서 다음의 주요 구성 요소로 이루어져 있다.

- 카이버 계약 : 이것은 주요 계약으로 사용자, 보유분 관리자를 위한 시스템의 주요 입구 역할을 한다.
- 사용자의 지갑 : 사용자를 지원하기위한 친숙한 인터페이스가 있는 지갑 응용 프로그램이다. 스테이터스, 토큰, 메타마스크과 같은 기존의 지갑 어플리케이션과의 통합은 카이버네트워크의 채택을 향상시키는데 도움이 될 것이다.
- 보유분 관리자 포털 : 그들의 성과, 네트워크 통계를 보여주고, 가격을 책정하고 재조정하는 여러 전략과 알고리즘들을 지원하는 기능으로써 보유금 관리에 도움을 준다. 보유금 관리자들은 이 포털을 통해 네트워크(또는 카이버 계약)와 상호작용 한다.
- 운영자 대시 보드 : 이는 카이버네트워크 운영자가 전체 시스템을 관리 할 수 있도록 도와준다. 운영자는 이 대시 보드를 통해 새로운 보유분을 추가 및 삭제하고, 네트워크 매개 변수를 변경할 수 있다.

2.4. 카이버네트워크 API 들

카이버네트워크는 사용자와 보유자와 보유분 기여자들을 위한 여러 API 명령들을 지원한다.

2.4.1. 사용자 API

사용자 API 는 일반 계좌와 계약을 포함하는 어떠한 이더리움 계좌에서도 호출될 수 있다.

Transfer(amount, source tokens, destination token name, destination address)
전송함수(금액, 소스 토큰, 대상 토큰 이름, 대상 주소)

전송 함수는 소스 토큰 (토큰 A)의 양을 대상 토큰 (토큰 B)으로 변환하고 유형 B 토큰을 대상 주소로 전송한다. 예를 들어, 사용자는 다음과 같이 전송 함수를 호출할 수 있다.
Transfer (100, "DGD", "Melon", "0xb794f5ea0ba39494ce839613fffba74279579268")
이를 수행하면 100 개의 디직스다오(DigixDAO) 토큰을 멜론포트(MelonPort) 토큰으로 변환하고 변환 된 모든 멜론포트 토큰을 "0xb794f5ea0ba39494ce839613fffba74279579268"의 주소로 전송한다.

GetExchangeRate(token A, token B)
환율받기함수 (토큰 A, 토큰 B)

이 함수를 호출하면 토큰 A 와 토큰 B 사이의 환율에 대한 값을 받는다. 장래에 우리는 서로 다른 거래량에 대한 다른 환율을 지원할 수 있다.

2.4.2. 보유분 기여자 API

보유분 기여자 API는 이더리움 네트워크의 모든 계좌에서 호출 할 수 있지만, 일부 API는 계좌가 이미 기여에 참여한 경우에만 작동한다. 카이버네트워크에는 두가지 타입의 보유분이 있다 : 공개 자금 기여를 받지 않는 개인 보유분과 공개 자금 기여를 허용하는 공개 보유분이 있다. 공개 보유분의 API들은 멜론펀드(멜론포트가 만든 분산화된 헷지 펀드 플랫폼)의 API와 매우 유사하다. 여기에 그 주요한 API들을 나열했다.

ContributeReserve(token type, amount)
보유분 기여 함수 (토큰 유형, 금액)
특정 토큰 유형의 일정양을 보유분에 기여하는 함수이다. 모든 기여 마다 기여자는 플랫폼에 대한 그들의 기여도를 나타내기 위해 일정량의 카이버네트워크 크리스탈(KNC)를 받게 될 것이다.

WithdrawProfits ()
이익인출함수()
이익은 기부자의 기여도에 비례하여 분배된다. 플랫폼 이익을 분배하기 위한 정확한 공식은 보유분의 구현에 따라 달려있을 것이다.

ContributeReserve(token type, amount)
기여인출함수 (KNC 금액, 토큰 유형)
기존 기부자는 보유분에서 그들의 기여금을 인출 할 수 있다. 기여자는 그가 인출 한 기여금에 대해 받고자 하는 토큰 유형을 명시 할 수 있으며 백그라운드에서 변환이 수행된다.

2.4.3. 보유분 관리자 API

SetRate(token A , token B, rate)
환율설정함수(토큰 A, 토큰 B, 환율)
기존 토큰 환전 쌍인 토큰 A와 토큰 B 사이의 환율을 설정하는 함수이다.
실제 적용되면, 이 API는 한 거래에서 모든 기존 환전 쌍의 환율을 업데이트하는 다른 API로 대체될 것이다. 이러한 총괄적 업데이트의 목적은 주로 가스 비용을 줄이는 데 있다.

2.4.4. 카이버네트워크 운영자 API

ListPair (token A, token B, initial rate)
토큰환전쌍목록추가함수(토큰 A, 토큰 B, 시작 환율)
카이버네트워크가 지원하는 목록에 토큰 A와 토큰 B의 새로운 토큰 환전 쌍 추가

DelistPair (token A, token B)
토큰환전쌍목록추가함수 (토큰 A, 토큰 B)
토큰 A와 토큰 B의 토큰 환전 쌍 거래 수락을 정지시킴

AddReserve (reserveAddress)
보유분추가함수 (보유분 주소)
네트워크에 새로운 보유분을 추가시킴. 추가된 보유분은 그 보유분의 관리자가 관리함.

RemoveReserve (reserveAddress)
보유분삭제함수 (보유분 주소)
카이버네트워크에서 기존 보유분을 삭제함. 보유분 삭제는 낮은 유동성과 나쁜 가격 및 기타 이유로 삭제된다.

2.5. 신용 확인 필요 없는 체인간 거래 지원

BTCRelay 와 같은 블록체인간 중계 플랫폼은 서로 다른 블록체인간의 통신을 가능하게 한다. 폴카닷이나 코스모스와 같은 프로토콜의 출시는 다른 블록체인간의 상호 작용을 더욱 쉽게 만들 것이다. 카이버네트워크는 이러한 기술들을 활용하여 이더리움 계좌로 서로 다른 암호화 화폐를 지불 받을 수 있도록 한다.

3. 시스템 특징

3.1. 신용 확인 필요 없음과 보안

카이버네트워크 운영자는 사용자의 토큰을 보유하지 않는다. 따라서 의도된 대로 사용자의 토큰은 도난으로부터 안전하게 보호된다. 스마트 컨트랙트에 의해 운영자의 무결성이 강화/보장되므로 사용자는 보유분 개체와 KNC 토큰 소유자들의 의도가 신뢰가 가는지에 대한 신용도를 신경 쓸 필요가 없다.

3.2. 즉각적인 거래

환전 또는 변환 요청은 단일 거래 내에서 즉시 실행된다. 사용자는 자신의 기존 토큰을 송금 한 순간에 즉각적으로 교환 된 토큰을 받는다. 보증금이나 확인 또는 대기 시간이 필요 없다. 이 효율적이고 사용자 친화적인 특징은 카이버네트워크를 다른 기존의 대부분과 미래에 생길 거래소와 구별되게 만든다.

3.3. 블록체인상 환전

환전은 블록체인을 통해 실행되며 일반 계좌 및 스마트 컨트랙트를 포함한 모든 계좌에서 액세스 할 수 있다. 따라서 스마트 컨트랙트는 제 3 자의 개입없이 환전하는 사람과 직접 상호 작용하여 기존에 지원하지 않는 다른 토큰으로 자금 지원 및 지불을 받을 수 있다. 이 기능을 통해 카이버네트워크는 일반 계좌 및 스마트 컨트랙트를 포함한 모든 계좌에 대한 블록체인 기반 프록시 지불 플랫폼이 된다.

3.4. 호환성

카이버네트워크는 이더리움의 기본 프로토콜과 기존의 스마트 컨트랙트 내에서 기능하도록 하기 위해 어떤 수정도 할 필요가 없다. 우리의 결제 API 는 그들 쪽에서 어떠한 변경 없이도 기존의 계약으로 통신할 수 있다.

이 말인즉슨, 우리는 모든 사용자 이더와 토큰들을 보유할 수 있는 새로운 계약 지갑을 도입한다는 것이다. 그 지갑을 사용하여 사용자가 토큰 A 로 토큰 B 를 지불할 계약을 체결할 수 있다. 여기서 A 에서 B 로의 변환은 카이버네트워크에서 원활하게 수행된다. 지불 받는 사람은 기존의 사용자가 보낸 것처럼 지불 받게 된다.

3.5. 기존 시스템과의 비교

아래는 카이버네트워크와 기존의 시스템과 비교한 표이다.

거래소	거래 비용[6]	신용 검증 필요 없는	즉각적인 거래	블록체인 상	보장된 유동성	적대적 공격에 대한 보안성

[6] 거래 수수료 및 별도로 거래를 실행하는데 발생하는 비용

크라켄/폴로닉	낮음	필요함	아님	아님	맞음	아님
쉐이프쉬프트	낮음	필요함	맞음	아님	맞음	아님
코인베이스	낮음	필요함	맞음	아님	맞음	아님
이더델타 오아시스 인덱스	높음	필요 없음	아님	맞음	아님	맞음
스왑.테크 제로엑스프로젝트	낮음 낮음	약간 필요함[7]	아님	혼용	아님	확실하지 않음[8]
카이버네트워크	낮음	필요 없음	맞음	맞음	맞음	맞음

4. 어플리케이션들

4.1. 즉각적이고 보안된 환전

가장 먼저 카이버네트워크는 거래소이다. 그러나 대부분의 거래소와는 다르게 카이버네트워크는 거래 요청을 즉각적으로 처리한다. 게다가 카이버네트워크는 사용자의 토큰을 보유하지 않으므로 어떠한 도난이나 분실도 설계상으로 방지되어 있다. 이것은 대개 거래 확정에 소요되는 몇 분의 거래 시간이 필요한 대부분의 거래소와 매우 대조적이다. 이 시간 동안의 오작동으로 불편을 겪거나 최악의 경우 자금 손실을 겪을 일이 없다.

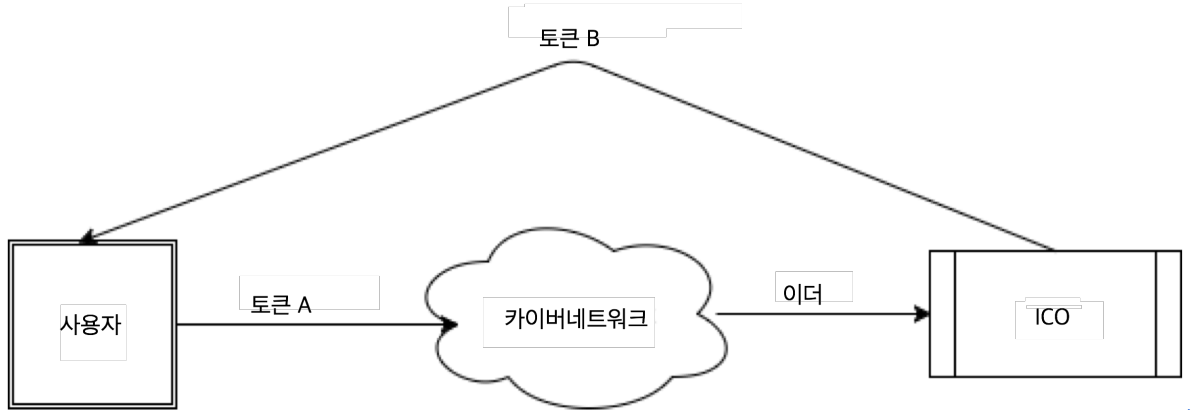
4.2. 모든 토큰으로 하는 공통의 거래 API 들

스마트 컨트랙트을 통한 환전을 통해 사용자는 어떠한 서비스나 제품도 그들이 선호하는 암호화 토큰으로 지불 할 수 있다. 이 계약은 이더에서의 즉각적인 변환을 제공하고 그가 원하는 모든 계약에 사용자를 대신하여 안전하게 지불한다. 아래 그림은 사용자가 이더만 받는 ICO 에 어떤 토큰으로도 참여할 수 있는 방법을 설명한다. 전체 프로세스는 단일 거래 내에서 발생하며 카이버네트워크는 절대 사용자 토큰(토큰 A 또는 토큰 B 모두)을 소유하지 않는다.

---

[7] 사용자는 최상의 거래 상대방을 찾는 중계자를 신뢰할 필요가 있다.

[8] 공격자들은 아무 비용을 들이지 않고 가짜 주문을 많이 생성해낼 수 있다. 이 상황에서는 거래가 제대로 될 수 있다는 보장이 없다.



4.3. 환전 비율에 대한 신뢰있는 블록체인상 소스

카이버네트워크의 환율은 다른 스마트 컨트렉트에서도 확인 가능하다. 따라서 스왑 계약과 같은 상위 금융 상품의 구현이 가능하다. 카이버네트워크에서 제공하는 호가는 두 토큰 사이를 거래하는 데 사용되는 실제 환율을 반영하므로 안전하다.

4.4. 가격변동 위험의 완화

암호화 자산의 유동성 부족으로 인해 환율은 불규칙한 수요와 공급으로 인해 너무 급변하는 것처럼 보인다. 기꺼이 자신의 자산을 보유고에 넣어두려 하는 시장 참가자가 부족하기 때문에 이 문제는 더욱 악화된다. 이제는 암호화 자산 사용자가 그들 스스로 미래 요구 사항에 대해 대비하기가 거의 불가능해졌다. 카이버네트워크는 사용자에게 더 많은 대안을 제공하기 위해 선도거래 및 옵션거래 형태로 파생 상품을 도입함으로써 이러한 문제를 해결할 것이다.

4.5. 선도거래

선도거래는 당사자들이 현재 지정된 가격으로 나중에 자산을 교환하는 것에 동의하는 계약이다. ICO 가 주류가 되는 상황에서 일반적인 문제 중 하나는 곧 시작 될 ICO 에 참여하기 위해 어떠한 사용자는 멜론에서 이더로 교환하듯이 토큰을 변환해야하는 것이다. 사용자는 현행 시장 가격으로 이더를 획득하거나 이더의 가격 변동 위험을 무효화 할 수 있는 선도 거래 계약을 체결 할 수 있다.

4.6. 옵션거래

옵션 계약을 통해 사용자는 프리미엄이라는 수수료로 불리한 가격 변동을 대비 할 수 있다. 콜 옵션은 계약 소유자에게 합의 된 가격으로 암호화 자산을 구입할 수 있는 권리를 준다. 풋 옵션은 그 반대이다. 프리미엄은 기본적인 암호화 자산의 내재 변동성을 사용하여 계산된다. 향후 구매 또는 판매 약정을 준비해야하는 암호화 자산 사용자는 콜이나 풋 옵션을 구매할 때 프리미엄을 지불 할 수 있다. 예를 들어 가격 변동이 없었던 토큰 소지자는 가격 상승을 포기하면서 프리미엄을 벌기 위해 콜 옵션을 작성할 수 있다.

5. 로드맵

카이버네트워크의 로드맵은 몇가지 단계가 포함되어 있다.

5.1. 0 단계 : 테스트넷 개발

예상 전달 시기 : 2017 년 8 월
카이버네트워크 지갑, 주요 카이버네트워크 계약 및 보유분 대시 보드를 포함한 우리의 플랫폼의 MVP 버전 개발. 이 단계의 목적은 모든 주요 기능 과 어플리케이션이 포함된 카이버네트워크의 기본 기능 버전을 만드는 것이다. MVP 는 공개적으로 공개 될 예정이며 관련 계약은 이더리움 테스트넷에 배포 및 테스트 될 예정이다.

5.2. 1 단계 : 기본 메인넷 개발

예상 전달 시기 : 2018 년 1 분기
우리는 메인 네트워크에 카이버네트워크의 첫 번째 버전을 배포한다. 우리는 이더와 모든 토큰 간에 거래 및 프록시 지불을 지원하는 것으로 시작한다. 우리의 보유분이 모든 거래를 제공하는 주보유분이 될 것 같지만, 그럼에도 불구하고 우리는 토큰 대주주와 다른 시장 제작자와 파트너 관계를 맺어 그들의 보유분을 카이버네트워크에 도입할 계획이다. 우리가 지원하는 토큰은 시장에서 수요가 높고 거래량이 많은 인기 토큰이 될 것이다.
우리는 또한 마이이더월렛(MyEtherWallet), 스테이터스(Status), 작스(Jaxx)와 같은 지갑 제공사와 협력하여 카이버네트워크의 핵심 기능을 구현할 것이다. 대부분의 사용자가 자신이 선호하는 지갑을 계속해서 사용하기 때문에 그 지갑들에 우리의 기능을 반영하는 것이 카이버네트워크의 채택을 늘리는 가장 좋은 방법이다.

5.3. 2 단계 : 임의의 토큰 교환쌍을 지원

예상 전달 시기 : 2018 년 2 분기
이 단계는 1 단계가 원활하게 구현됨에 따라 쉽게 달성 될 수 있다. 그때까지 우리는 더 많은 보유자들(즉, 마켓 메이커)이 카이버네트워크에 참여할 것으로 기대한다. 우리의 플랫폼에서 더 많은 보유분을 확보 할 수 있음에 따라 지원하는 토큰들의 종류가 늘어난다. 또한 카이버네트워크는 다른 전략적 파트너와 협력하여 사용자가 그들의 플랫폼에서 선호하는 토큰으로 토큰/나눠진 수수료를 효율적으로 인출 할 수 있도록 API 를 구축한다. 예를 들어, 많은 플랫폼과 프로젝트는 수수료 공유 모델을 사용한다. 이것은 토큰 보유자가 플랫폼 사용자로부터 모은 모든 플랫폼 사용료(많은 토큰으로 확산될 수 있는)를 나누는 것이다. 이 플랫폼들이 카이버네트워크의 연관된 API 들을 쓴다면 이 플랫폼들의 토큰 보유자들은 그들의 몫의 수수료를(예를 들면 이더로) 원활하게 받을 수 있을 것이다.

5.4. 3 단계 : 상위 금융 상품 거래

예상 전달 시기 : 2018 년 4 분기
우리의 개발 및 운영이 안정화되면 카이버 네트워크의 3 단계를 전개 할 것이며, 여기서는 4 장에서 논의한 바와 같이 상위의 금융 상품 거래를 지원한다. 우리는 사람들이 신용 검증 필요 없는 헤지 펀드에 투자하고 효율적인 펀드 관리를 통해 이익 분배를 얻을 수 있게 해주는 분산화된 헤지 펀드 플랫폼(예. 멜론포트에 의해 제공된)과 협력 할 계획이다. 우리 팀은 안전한 방법으로 목표를 달성 할 수 있도록 하는 관련 플랫폼간의 API 를 만들고 환전하는 것에 대한 논의가 필요하다. 마찬가지로 그들의 창업자와 고문들을 위한 베스팅 계획을 가지는 ICO 프로젝트들과의 협업도 중요하다.

5.5. 4 단계 : 다른 블록체인간의 거래 지원

예상 전달 시기 : 2018 년 말/ 2019 년 초

이 단계의 배포로 사용자는 이더/토큰들과 비트코인(Bitcoin), 지캐쉬(ZCash), 이더리움클래식(ETC) 등과 교환 할 수 있다. 이 목표를 달성하는 법에는 다음 두가지가 있다. 체인 중계를 사용하는 방법(예. BTCRelay 및 ZecRelay) 또는 체인내 통신 프로토콜(예. 코스모스, 폴카닷)을 사용하는 방법이다. 카이버네트워크에서 이 중 어떤 솔루션을 사용할 것인지 결정하기 위해 이 프로토콜과 릴레이의 개발을 면밀히 관찰 할 것이다.,

6. 감사의 글

우리는 다음 사람들에게 감사를 전한다. 우리의 고문인, 웡 리 홍(Wong Lee Hong), 비탈릭 부테린(Vitalik Buterin), 렝 호에 론(Leng Hoe Lon), 프라틱 색세나(Prateek Saxena) 그리고 우리의 친구들인 춘 응아이 리(Tsun Ngai Lee), 스텔리안 발타(Stelian Balta), 레토 트링클러(Reto Trinkler). 이 백서의 초창기 버젼의 피드백에 대해 감사 인사를 전한다.

7. 팀 구성원

7.1. 핵심 멤버들

1. **로이 루(Loi Luu)**
   로이 루는 암호화 화폐, 스마트 컨트랙트 보안 및 분산 된 합의 알고리즘을 연구하는 연구원이다. 그의 연구 보고서는 온라인에서 볼 수 있으며 데브콘 2(DevCon2), 에드콘(EdCon), 스케일링 비트코인(Scaling Bitcoin)과 같은 비트코인과 이더리움 워크숍에서 정기적으로 초청 연사로 활동하고 있다. 로이는 이더리움과 블록체인 기술의 힘을 믿는다. 그의 일의 상당 부분이 이 커뮤니티를 중심으로 이루어진다. 그는 이더리움 스마트 계약을 위한 최초의 오픈 소스 보안 분석기인 오이엔테(Oyente)를 개발했다. 다음으로, 그는 또 다른 오픈 소스 프로젝트인 기존의 암호화 화폐의 채광 풀의 분산화를 수용하는 스마트풀(SmartPool)을 공동 설립했다. 그는 블록체인 커뮤니티를 위해 가치를 개발하고 영감을 얻으면서 카이버네트워크를 통해 계속해서 분산화와 신용 검증 없는 특성을 지닌 블록체인을 옹호하고 있다.

2. **야론 벨르너(Yaron Velner)**
   야론 벨르너는 스마트풀(SmartPool) 프로젝트의 공동 창립자이자 연구원이다. 그의 연구는 블록 체인 프로토콜에서 보상에 대한 게임 이론 측면과 스마트 컨트랙트의 공식 검증에 초점을 두고 있다. 그는 텔아비브 대학(Tel Aviv University)에서 컴퓨터 과학 박사 학위를 취득했다. 그의 박사 학위 논문에서 그는 게임 이론 기술을 컴퓨터 프로그램 및 시스템의 공식 검증에 대한 어플리케이션을 연구했다. 야론은 또한 이지칩(EZchip) 반도체(최근 멜라녹스 테크놀로지로 인수 됨)에서 선임 소프트웨어 엔지니어 및 기술 리더로서 10 년 이상의 경력을 쌓은 경험 많은 소프트웨어 개발자이다. 이지칩에서 그는 IP 라우팅을 위한 새로운 데이터 구조를 개발 한 데이터 구조 및 알고리즘 팀의 멤버였다.

3. **빅터 트란(Victor Tran)**
   빅터 트란은 선임 백엔드 엔지니어이자 리눅스(Linux) 시스템 관리자이다. 그는 다중 소셜 마케팅 플랫폼 및 광고 네트워크를 위한 인프라를 개발하고 구축 한 경험이 있다. 그는 고성능 멀티 플랫폼 애플리케이션을 개발하는 데 관심이 있다. 빅터는 소셜 마케팅 분야의 여러 스타트업을 공동 창립하고 CTO 를 지 냈다. 그는 월간 수백만 명의 활성

유저를 처리하는 플랫폼을 구축하고 유지 관리했다. 빅터는 현재 스마트풀(SmartPool) 프로젝트의 수석 엔지니어이다.

4. 쿠옹 응우엔(Cuong Nguyen)

쿠옹은 몇 년 동안 흥미로운 웹 응용 프로그램을 만든 수석 웹 개발자이다. 그는 최근 비트코인, 이더리움 및 IBM의 패브릭 레저(Fabric ledger)를 비롯한 다양한 블록 체인 플랫폼을 실험하는 데 대부분의 시간을 보내고 있다.

7.2. 고문들

1. 웡 리 홍(Wong Lee Hong)

웡 리 홍의 경력은 30 년 이상 다양한 산업 분야에 걸쳐 있다. 그는 소비자 전자, 멀티미디어, 컴퓨터 게임, 인터넷 및 금융 분야에서 광범위한 유통 및 사업 개발 경험을 보유하고 있다. 그의 경력의 후반부에는 주요 금융 기관의 인터넷 뱅킹 역량, 전략적 스타트업의 벤처 캐피탈 활동 및 규제 관리 역할을 개발하고 은행 기술 및 운영과 관련한 주요 문제에 대해 아시아의 은행 규제 기관들을 다루는 일을 주로 했다. 현재 그는 블록 체인 열성 지지자이자 투자자이다.

2. 렝 호에 론(Leng Hoe Lon)

렝 호에 론은 싱가포르 국립 대학교(National University of Singapore)와 공동으로 최신 데이터 기반 기술을 사용하여 사업 결정을 내리고 경쟁 우위를 확보하는 것을 목표로 하는 쉔틸리움(Shentilium)을 설립했다. 그는 또한 누구나 전문적인 위험 관리 프레임워크 내에서 수익성 있는 금융 시장 거래를 배울 수 있다는 비전을 바탕으로 트랙레코드 아시아(TrackRecord Asia)를 공동 창립했다. 그 전에는 도이체 방크(Deustsche Bank) - 런던 및 싱가포르, 제이피모건(JPMorgan) - 싱가포르, 아비엔 아므로(ABN Amro) - 싱가포르 등 금융 업계에서 다양한 직책을 수행했다. 그는 홍콩의 골드만 삭스(Goldman Sachs) 아시아 매크로 트레이딩 그룹의 전무 이사 겸 런던의 아시안 FX 트레이더였다. 그는 또한 세계 거시 헤지 펀드인 튜더 캐피탈 싱가프로(Tudor Capital Singapore)의 CEO 이기도 했다.

3. 프라틱 색세나(Prateek Saxena)

프라틱 색세나는 싱가포르 국립 대학교(National University of Singapore)의 컴퓨터 과학 연구 교수이다. 그는 블록체인과 컴퓨터 보안 분야에서 일하고 있다. 그의 연구는 오늘날 널리 사용되는 브라우저 플랫폼, 웹 표준 및 앱 스토어의 디자인에 영향을 미쳤다. 그는 MIT TR35 Asia 와 같은 여러 주요 수상의 영예를 안았다.

4. 비탈릭 부테린(Vitalik Buterin)

비탈릭은 이더리움의 설립자이자 수석 과학자이다. 그는 또한 비트코인 매거진의 설립자이자 작가이기도 하며, 2011 년에 암호화계에서 경력을 쌓기 시작했다. 그는 안전하고 효율적이며 신뢰할 수 있는 시스템을 만드는 데 관심이 있으며 암호화 분야에서 많은 프로젝트에 대해 조언하고 있다.